WHAT IS CLAIMED IS:

1. A system for preventing tampering with recorded accumulated running distance data, comprising:

a first memory unit being provided in a cluster and being configured to store accumulated running distance data;

a tampering prevention control unit with a second memory unit and being configured to receive input vehicle serial number data and to store the vehicle serial number data in the second memory unit and the first memory unit, and being configured to receive the accumulated running distance data and to store the received accumulated running distance data in the second memory unit; and

a third memory unit being provided in an engine control unit and receiving the vehicle serial number data and the accumulated running distance data from the tampering prevention control unit and storing the received vehicle serial number data and the accumulated running distance data,

wherein the tampering prevention control unit is configured to output an error message if the vehicle serial number data stored in the second memory unit is not equal to the vehicle serial number data stored in the first memory unit and the third memory unit,

and wherein the tampering prevention control unit is configured to determine whether the accumulated running distance data stored in the second memory unit is equal to the accumulated running distance data stored in the first memory unit, and if not, the tampering prevention control unit causes the accumulated running distance data stored in the second memory unit to be stored in the first memory unit.

2. The system of claim 1, wherein the tampering prevention control unit further comprises a coding module for coding the input vehicle serial number data to produce coded vehicle serial number data which is stored respectively in the second memory unit, the first memory unit, and the third memory unit.

3. The system of claim 1, wherein each of the first memory unit, the second memory unit, and the third memory unit is a memory device in which data can be stored and from which data can be deleted.

4. The system of claim 1, wherein the tampering prevention control unit further comprises an input interface through which the vehicle serial number data is input.

5. A method for preventing tampering with recorded accumulated running distance data, comprising:

storing input vehicle serial number data in a tampering prevention control unit, a cluster, and an engine control unit, and setting accumulated running distance data;

outputting an error message if the vehicle serial number data stored in the tampering prevention control unit is not equal to the vehicle serial number data stored in the cluster and the vehicle serial number data stored in the engine control unit, in an ignition-on state; and

displaying an accumulated running distance stored in the cluster if the accumulated running distance data stored in the cluster is equal to the accumulated running distance data stored in the tampering prevention control unit, and storing the accumulated running distance data stored in the tampering prevention control unit to the cluster and displaying the accumulated running distance data stored in the tampering prevention control unit if the accumulated running distance data stored in the cluster is not equal to the accumulated running distance data stored in the tampering prevention control unit.

6. The method of claim 5, wherein the input vehicle serial number data is coded to produce a coded vehicle serial number data which is stored in the tampering prevention control unit, the cluster, and the engine control unit.

7. The method of claim 5, further comprising causing the accumulated running distance data stored in the cluster to be stored in the tampering prevention control unit and the engine control unit upon turning off the ignition.